Amendments to the Claims:

This listing of claims will replace all prior versions, and listing, of claims in the application:

Listing of Claims:

1. (currently amended) A method for detecting and preventing security breaches in a network, the method comprising:

reassembling a plurality of TCP packets in network traffic into a TCP stream;

grouping the plurality of TCP packets into packet flows and sessions;

storing the packet flows in packet flow descriptors, the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type;

inspecting the TCP stream to detect information indicative of a security breach;

dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach;

forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach,

wherein inspecting the TCP stream to detect information indicative of a security breach comprises:

storing a plurality of protocol specifications supported by the network in a protocol database,

querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database, and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream.

2. (original) The method of claim 1, wherein inspecting the TCP stream to detect information indicative of security breaches comprises inspecting the TCP stream for protocol irregularities.

3. (previously presented) The method of claim 1, wherein inspecting the TCP stream to detect information indicative of a security breach comprises searching the TCP stream for attack signatures.

4. (original) The method of claim 3, wherein searching the TCP stream for attack signatures comprises using stateful signature detection.

5. (previously presented) The method of claim 1, wherein inspecting the TCP stream to detect information indicative of a security breach comprises using a plurality of network intrusion detection methods.

6. (original) The method of claim 5, wherein the plurality of network intrusion detection methods comprises at least protocol anomaly detection.

7. (original) The method of claim 5, wherein the plurality of network intrusion detection methods comprises at least signature detection.

8. (canceled)

9. (canceled)

10. (previously presented) The method of claim 1, further comprising searching the packet flow descriptors for traffic signatures.

11. (canceled)

12. (previously presented) The method of claim 1, wherein the network attack identifier comprises a protocol irregularity.

13. (previously presented) The method of claim 1, wherein the network attack identifier comprises an attack signature.

14. (previously presented) The method of claim 1, wherein the network attack identifier comprises a plurality of network attack identifiers.

15. (original) The method of claim 14, wherein the plurality of network attack identifiers comprises at least a protocol irregularity.

16. (original) The method of claim 14, wherein the plurality of network attack identifiers comprises at least an attack signature.

17. (previously presented) The method of claim 13, wherein the attack signature and traffic signatures are stored in a signatures database.

18. (currently amended) A method comprising:

reassembling a plurality of TCP packets into a TCP stream;

inspecting the TCP stream to detect information indicative of a security breach;

dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach;

forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach; and

grouping the plurality of TCP packets into packet flows and sessions, wherein grouping the plurality of TCP packets into packet flows and sessions comprises storing the packet flows and sessions in a hash table,

wherein inspecting the TCP stream to detect information indicative of a security breach comprises:

storing the packet flows in packet flow descriptors, and

searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream, wherein storing the packet flows and sessions in a hash table comprises computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type.

19. (canceled)

20. (canceled)

21. (previously presented) The method of claim 3, wherein searching the TCP stream for attack signatures comprises querying a signatures database to determine whether there are matching signatures in the TCP stream.

22. (previously presented) A method for detecting and preventing security breaches in a network, the method comprising:

reassembling a plurality of TCP packets into a TCP stream;

inspecting the TCP stream to detect information indicative of a security breach;

dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach;

forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach, wherein inspecting the TCP stream to detect information indicative of a security breach comprises:

querying a signatures database to determine whether there are matching signatures in the TCP stream using deterministic finite automata for pattern matching.

23. (original) The method of claim 1, further comprising reconstructing the plurality of TCP packets from a plurality of packet fragments.

24. (currently amended) A system for detecting and preventing security breaches in a network, the system comprising:

a TCP reassembly software module for reassembling a plurality of TCP packets in network traffic into a TCP stream;

a software module for inspecting the TCP stream to detect information indicative of a security breach;

a software module for dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach;

a software module for forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach[[,]]; and

at least one processing device configured to execute the TCP reassembly software module, the software module for inspecting the TCP stream, the software module for dropping a TCP packet and the software module for forwarding a TCP packet,

wherein the software module for inspecting the TCP stream comprises at least a protocol anomaly detection software module and a flow manager software module, the protocol anomaly detection software module comprising:

a routine for storing a plurality of protocol specifications supported by the network in a protocol database, and

a routine for querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database,

wherein the flow manager software module is configured to:

group the plurality of TCP packets into packet flows and sessions,

store the packet flows in packet flow descriptors, the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type, and

search for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream.

25. (original) The system of claim 24, further comprising an IP defragmentation software module for reconstructing a plurality of packet fragments into the plurality of TCP packets.

26. (canceled)

27. (currently amended) A system comprising:

a TCP reassembly software module for reassembling a plurality of TCP packets network traffic into a TCP stream;

a software module for inspecting the TCP stream to detect information indicative of a security breach;

a software module for dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach;

a software module for forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach; ~~and~~

a flow manager software module for grouping the plurality of TCP packets into packet flows and sessions, wherein the flow manager software module comprises a routine for storing the packet flows and sessions into a hash table, storing the packet flows in packet flow descriptors, and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream; and

at least one processing device configured to execute the TCP reassembly software module, the software module for inspecting the TCP stream, the software module for dropping a TCP packet, a software module for forwarding a TCP packet and the flow manager software module,

wherein the routine for storing the packet flows and sessions into a hash table comprises a routine for computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type.

28-30. (canceled)

31. (previously presented) The system of claim 24, wherein the software module for inspecting the TCP stream to detect information indicative of a security breach comprises a stateful signature detection software module.

32. (previously presented) The system of claim 27, further comprising a traffic signature detection software module for searching the packet flow descriptors for traffic signatures.

33. (previously presented) The system of claim 24, wherein the software module for inspecting the TCP stream for information indicative of a security breach comprises a plurality of software modules.

34. (canceled)

35. (original) The system of claim 33, wherein the plurality of software modules comprises at least a stateful signature detection software module.

36. (canceled)

37. (previously presented) The system of claim 24, wherein the protocol specifications comprise specifications of one or more of: TCP protocol; HTTP protocol; SMTP protocol; FTP protocol; NETBIOS protocol; IMAP protocol; POP3 protocol; TELNET protocol; IRC protocol; RSH protocol; REXEC protocol; and RCMD protocol.

38. (original) The system of claim 35, wherein the stateful signature detection software module comprises a routine for querying a signatures database to determine whether there are matching attack signatures in the TCP stream.

39. (currently amended) A system for detecting and preventing security breaches in a network, the system comprising:

a TCP reassembly software module for reassembling a plurality of TCP packets in network traffic into a TCP stream;

a software module for inspecting the TCP stream to detect information indicative of a security breach;

a software module for dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach; ~~and~~

a software module for forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach, wherein the software module for inspecting the TCP stream to detect information indicative of a security breach comprises a stateful signature detection software module, the stateful signature detection software module comprising:

a routine for querying a signatures database to determine whether there are matching attack signatures in the TCP stream using deterministic finite automata for pattern matching; and

at least one processing device configured to execute the TCP reassembly software module, the software module for inspecting the TCP stream, the software module for dropping a TCP packet and the software module for forwarding a TCP packet.

40. (previously presented) The system of claim 24, further comprising:

a routine for collecting a plurality of security logs and alarms recording information about security breaches found in the TCP stream;

a routine for storing a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented;

a routine for distributing the network security policy to one or more gateway points in the network; and

a routine for updating the protocol database and a signatures database.

41. (original) The system of claim 24, further comprising a graphical user interface comprising:

a routine for displaying network security information to network security administrators; and

a routine for specifying a network security policy.

42. (currently amended) A system for detecting and preventing security breaches in a network, the system comprising:

a network intrusion detection and prevention sensor located in a network gateway, wherein the network intrusion detection and prevention sensor ~~comprises~~ including at least one processor configured to execute:

a routine for reassembling a plurality of TCP packets into a TCP stream;

a software module for inspecting the TCP stream to detect information indicative of a security breach, wherein inspecting the TCP stream to detect information indicative of a security breach comprises:

storing a plurality of protocol specifications supported by the network in a protocol database, and

querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database;

a software module for dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach; and

a software module for forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach;

a central management server to control the network intrusion detection and prevention sensor; and

a graphical user interface for configuring the network intrusion detection and prevention sensor,

wherein the network intrusion detection and prevention sensor further comprises a flow manager software module and a traffic signature detection module, the flow manager software module being configured to:

group the plurality of TCP packets into packet flows and sessions, and

store the packet flows in packet flow descriptors, the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type, and

the traffic signature detection module is configured to:

search for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream.

43. (previously presented) The system of claim 42, wherein the network intrusion detection and prevention sensor is located within a firewall.

44. (previously presented) The system of claim 42, wherein the network intrusion detection and prevention sensor is located outside a firewall.

45. (original) The system of claim 42, wherein the network intrusion detection and prevention sensor further comprises an IP defragmentation software module for reconstructing a plurality of packet fragments into the plurality of TCP packets.

46. (previously presented) The system of claim 42, wherein the network intrusion detection and prevention sensor further comprises an IP router software module for routing a TCP packet from the TCP stream if the TCP stream does not contain information indicative of a network security breach through the network.

47. (canceled)

48. (canceled)

49. (previously presented) The system of claim 42, wherein the software module for inspecting information indicative of a security breach comprises a protocol anomaly detection software module.

50. (previously presented) The system of claim 42, wherein the software module for inspecting information indicative of a security breach comprises a stateful signature detection software module.

51. (canceled)

52. (previously presented) The system of claim 42, wherein the software module for inspecting information indicative of a security breach comprises a plurality of software modules.

53. (original) The system of claim 52, wherein the plurality of software modules comprises at least a protocol anomaly detection software module.

54. (original) The system of claim 52, wherein the plurality of software modules comprises at least a stateful signature detection software module.

55. (original) The system of claim 42, wherein the central management server comprises:

a routine for collecting a plurality of security logs and alarms recording information about security breaches found in the TCP stream;

a routine for storing a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented; and

a routine for distributing the network security policy to the network intrusion detection and prevention sensor.

56. (original) The system of claim 42, wherein the graphical user interface comprises:

a routine for displaying network security information to network security administrators;

a routine for displaying status information on the network intrusion detection and prevention sensor; and

a routine for specifying a network security policy.

57. (currently amended) A network intrusion detection and prevention sensor for detecting and preventing network security breaches at a network gateway, the network intrusion detection and prevention sensor comprising:

a flow manager software module for grouping a plurality of packets into packet flows and sessions;

a TCP reassembly software module for reassembling a plurality of TCP packets from the plurality of packets into a TCP stream;

a software module for inspecting the TCP stream according to the packet flows and sessions to detect information indicative of a security breach, wherein inspecting the TCP stream to detect information indicative of a security breach comprises:

storing a plurality of protocol specifications supported by the network in a protocol database, and

querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database;

a software module for dropping a packet from the plurality of packets if the TCP stream contains information indicative of a security breach;

a software module for forwarding a packet from the plurality of packets to a network destination if the TCP stream does not contain information indicative of a security breach;

a software module for grouping the plurality of TCP packets into packet flows and sessions and storing the packet flows in packet flow descriptors, the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type; ~~and~~

a software module for searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream; and

at least one processing device configured to execute the flow manager software module, the TCP reassembly software module, the software module for inspecting the TCP stream, the software module for dropping a packet, a software module for forwarding a packet, a software module for grouping the plurality of TCP packets and the software module for searching for a network attack identifier.

58. (original) The network intrusion detection and prevention sensor of claim 57, further comprising an IP defragmentation software module for reconstructing a plurality of packet fragments into the plurality of TCP packets.

59. (previously presented) The network intrusion detection and prevention sensor of claim 57, wherein the network intrusion detection and prevention sensor further comprises an IP router software module for routing a TCP packet from the TCP stream if the TCP stream does not contain information indicative of a network security breach through the network.

60. (original) The network intrusion detection and prevention sensor of claim 57, wherein the network intrusion detection and prevention sensor is controlled by a network

security policy specifying the network traffic to inspect and a plurality of network attacks to be detected and prevented.

61. (original) The network intrusion detection and prevention sensor of claim 60, wherein the network security policy is defined by a network security administrator using a graphical user interface.

62. (previously presented) The network intrusion detection and prevention sensor of claim 61, wherein the graphical user interface comprises:

a routine for displaying network security information to network security administrators;

a routine for displaying status information on the network intrusion detection and prevention sensor; and

a routine for specifying the network security policy.

63. (original) The network intrusion detection and prevention sensor of claim 60, wherein the security policy is stored and distributed to the network intrusion detection and prevention sensor by a central management server.

64. (original) The network intrusion detection and prevention sensor of claim 63, wherein the central management server comprises a routine for collecting a plurality of security logs and alarms recording information about security breaches found in the TCP stream.

65. (previously presented) The network intrusion detection and prevention sensor of claim 57, wherein the software module for inspecting the TCP stream according to the packet flows and sessions to detect information indicative of a security breach comprises a protocol anomaly detection software module.

66. (previously presented) The network intrusion detection and prevention sensor of claim 57, wherein the software module for inspecting the TCP stream according to the packet flows and sessions to detect information indicative of a security breach comprises a stateful signature detection software module.

67. (previously presented) The network intrusion detection and prevention sensor of claim 58, wherein the software module for inspecting the plurality of packets according to the packet flows and sessions to detect information indicative of a security breach comprises a plurality of software modules.

68. (original) The network intrusion detection and prevention sensor of claim 67, wherein the plurality of software modules comprises at least a protocol anomaly detection software module.

69. (original) The network intrusion detection and prevention sensor of claim 67, wherein the plurality of software modules comprises at least a stateful signature detection software module.